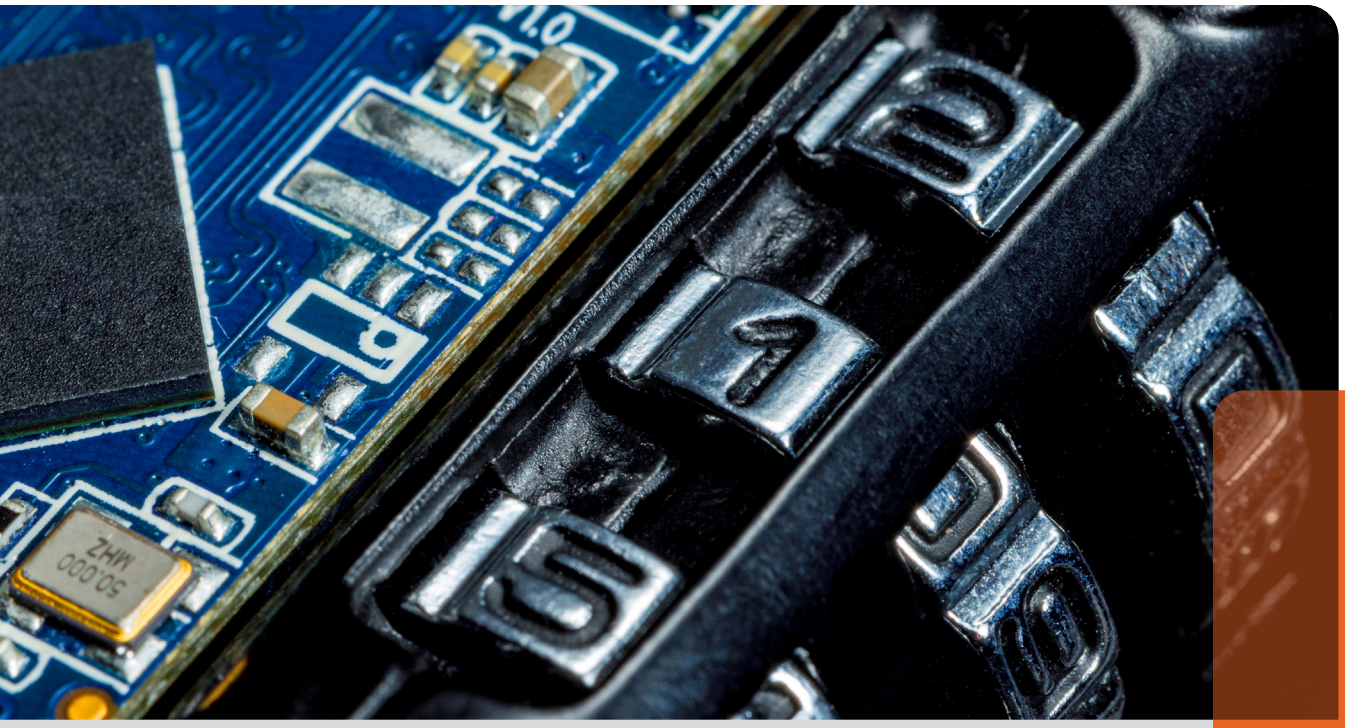
International
Comparative
Legal Guides



Data Protection

2024

11th Edition

Contributing Editors:
Tim Hickman & Detlev Gabel
White & Case LLP

glg Global Legal Group

Expert Analysis Chapters

Q&A Chapters

Ireland


Victor Timon


Zelda Deasy


Seán O'Donnell


Mark Condy

ByrneWallace LLP

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

Since 25 May 2018, the principal data protection legislation in the EU has been Regulation (EU) 2016/679 (the "**General Data Protection Regulation**" or "**GDPR**"). The GDPR repealed Directive 95/46/EC and has led to increased (though not total) harmonisation of data protection law across the EU Member States. The Data Protection Act 2018, as amended (the "**DPA 2018**") transposes the GDPR into national law in Ireland. The former Data Protection Acts 1988 to 2003 still apply in certain circumstances, such as to the processing of personal data for the purposes of safeguarding the security of the State.

1.2 Is there any other general legislation that impacts data protection?

The European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011, as amended (the "**ePrivacy Regulations**"), transpose Directive 2002/58/EC (the "**ePrivacy Directive**") into law. The ePrivacy Regulations outline specific rules with regard to the use of cookies, marketing communications and security of electronic communications networks and services. The ePrivacy Regulations were amended by the European Union (Electronic Communications Code) Regulations 2022, which broadened the range of service providers falling within the scope of the legislative requirements. The revised ePrivacy Regulation is still in draft at this stage and it is unclear when it will be finalised.

Further, EU Directive 2016/680 specifically regulates the processing of data by police and criminal justice authorities in the EU, such as *An Garda Síochána*, the Irish police force. The Directive requires the data collected by law enforcement authorities to be processed lawfully and fairly.

1.3 Is there any sector-specific legislation that impacts data protection?

The Data Sharing and Governance Act 2019 (the "**DSGA**") serves as a comprehensive framework for managing personal data within the public sector. It: (i) regulates the sharing of information, including personal data, between public bodies; (ii) provides for the establishment of base registries and implements the Personal Data Access Portal; and (iii) establishes the Data Governance Board, which is tasked with overseeing compliance, setting standards and promoting best practices in data governance across public entities.

Regulation (EU) 2022/2065 on a Single Market for Digital Services (the "**Digital Services Act**" or "**DSA**") came into effect in November 2022. The DSA applies to certain entities that provide an online "intermediary service" within the EU, and it builds on some of the well-established themes underpinning the GDPR. The DSA is enforced by the European Commission and "Digital Services Coordinators", to be designated by each Member State. Ireland has designated *Comisiún na Meán* as the Irish Digital Services Coordinator and the Competition and Consumer Protection Commission as a competent authority for online marketplaces. In the event of non-compliance with the DSA, service providers could receive fines of up to 6% of their annual global turnover.

The Digital Markets Act ("**DMA**") came into effect on 1 November 2022 and regulates designated "gatekeepers" of "core platform services" from imposing unfair conditions on businesses and end users, and ensures the openness of important digital services. The DMA applies to companies that exceed certain financial and market share thresholds and operate in certain digital sectors, including advertising services, online search engines, social networking services, online intermediary services, app stores, certain messaging services, virtual assistants, web browsers and operating systems.

The Policing, Security and Community Safety Act 2024, was signed into law on 7 February 2024, and empowers *An Garda Síochána*, the Authority (*An tÚdarás Póilíneachta agus Sábháilteachta Pobail*), and the Police Ombudsman to share data, including personal data, with other agencies to perform their functions.

1.4 What authority(ies) are responsible for data protection?

Each EU Member State appoints a dedicated national supervisory authority which is responsible for enforcement and oversight of data protection legislation within its jurisdiction. The Data Protection Commission ("**DPC**") is the national competent authority for the regulation and enforcement of the GDPR, the DPA 2018 and the ePrivacy Regulations in Ireland.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**" means any information relating to an identified or identifiable natural person; an identifiable

natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

- "**Processing**" means any operation or set of operations that is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- "**Controller**" means the natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data.
- "**Processor**" means a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller.
- "**Data Subject**" means an identified or identifiable natural person.
- "**Identified or identifiable natural person**" means a natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- "**Special-category Personal Data**" also known as "Sensitive Personal Data" are personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life and sexual orientation, genetic data or biometric data.
- "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
- "**Consent**" means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
- "**Cross-border Processing**" means either: (i) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the EU where the controller or processor is established in more than one Member State; or (ii) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the EU, but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

3 Territorial and Material Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The GDPR applies to businesses that are established in any EU Member State, and that process personal data (both as a controller or processor, and regardless of whether or not the processing takes place in the EU). The GDPR also applies to businesses outside the EU if they (either as controller or processor) process the personal data of EU residents in relation to: (i) the offering of goods or services (whether or not in return for payment) to EU residents; or (ii) monitor the behaviour of EU residents (to the extent that such behaviour takes place in the EU).

3.2 Do the data protection laws in your jurisdiction carve out certain processing activities from their material scope?

The GDPR applies where a controller or processor has an establishment in any EU Member State, and they process personal data in the context of that establishment, whether or not the processing takes place in the EU or not.

Controllers not established in the EU, but in a place where Member State law applies by virtue of public international law, are subject to the GDPR.

Controllers and/or processors who process personal data of data subjects who are in the EU, although the controllers and/or processors are outside the EU, will be subject to the GDPR where the processing activities are related to: (i) the offering of goods or services, irrespective of whether a payment by the data subject is required; or (ii) the monitoring of data subjects' behaviour as far as their behaviour takes place within the EU.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Lawfulness, fairness and transparency**.
  Personal data should be processed lawfully, fairly and in a transparent manner in relation to the data subject.
- **Lawfulness**
  Controllers must rely on one of six permitted lawful bases when processing personal data: (i) the consent of the data subject; (ii) necessity for the performance of a contract with the data subject; (iii) compliance with a legal obligation of the controller; (iv) necessity for the protection of the vital interests of the data subject or another natural person; (v) necessity for the performance of a task carried out in the public interest or an official function vested in the controller; and (vi) necessity for the legitimate interests of the controller or a third party, except where those interests are overridden by the interests or rights and freedoms of the data subject.
  The processing of special-category personal data is generally prohibited with 10 exceptions provided for in the GDPR where processing is permitted, such as: (i) with the consent of the data subject; (ii) where processing is necessary for the establishment, exercise or defence of a legal claim; or (iii) where processing is necessary to protect the vital interest of the data subject.
- **Fairness**
  This principle is not defined in the GDPR; however, the European Data Protection Board ("**EDPB**") has stated that it means personal data must not be "processed in a way that is detrimental, discriminatory, unexpected or misleading to the data subject". Data subjects should, therefore, be sufficiently informed as to how their personal data will be processed.
- **Transparency**
  Controllers must process personal data in a transparent manner and are obliged to furnish data subjects with

certain minimum information regarding the collection and processing of their personal data. This information should be concise, transparent, intelligible and in an easily accessible form, and use clear and plain language.

- **Purpose limitation**
  Personal data must only be collected for specified, explicit and legitimate purposes and not be further processed in a manner that is incompatible with those purposes. Where the controller wishes to further process the personal data in a manner that is incompatible with the original purposes of collection, the controller must inform the data subject of the further processing and rely on an appropriate lawful basis for processing.
- **Data minimisation**
  Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed.
- **Accuracy**
  Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- **Storage limitation**
  Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods solely for archiving purposes in the public interest, for scientific or historical research purposes or statistical purposes.
- **Integrity and confidentiality**
  Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- **Accountability**
  The controller is responsible for, and must be able to demonstrate, compliance with the data protection principles set out above.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to copies of data/information on processing**
  A data subject has the right to obtain from a controller the following information in respect of the data subject's personal data: (i) confirmation of whether, and where, the controller is processing the data subject's personal data; (ii) information about the purposes of the processing; (iii) information about the categories of data being processed; (iv) information about the categories of recipients with whom the data may be shared (note that the Court of Justice of the EU ruled in the *PostAG* (Case C-154/21) that the data subject is entitled to request the actual identities of recipients (not merely the categories) unless this is impossible); (v) information about the period for which the data will be stored (or the criteria used to determine that period); (vi) information about the existence of the rights to erasure, rectification, restriction of processing and to object to processing; (vii) information about the existence of the right to complain to the relevant data protection authority; (viii) where the data were not collected from the data subject, information as to the source of the data; and (ix) information about the existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on the data subject.
  The data subject may request a copy of the personal data being processed. The copy should include, *inter alia*, the purposes of processing, the categories of personal data processed and the envisaged period for which the personal data will be stored. This right must not adversely affect the rights and freedoms of others.
- **Right to rectification of errors**
  Data subjects may oblige controllers to rectify inaccurate personal data concerning them without undue delay. Rectification includes the completion of incomplete personal data, which may be updated by providing a supplementary statement.
- **Right to erasure ("the right to be forgotten")**
  Data subjects have the right to erasure of their personal data without undue delay if: (i) the data are no longer needed for their original purpose (and no new lawful purpose exists); (ii) the lawful basis for the processing is the data subject's consent, the data subject withdraws that consent, and no other lawful basis applies; (iii) the data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing; (iv) the data have been processed unlawfully; (v) erasure is necessary for compliance with EU law or national data protection law; or (vi) the data have been collected in relation to the offer of information society services.
- **Right of objection**
  Data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data where the basis for that processing is either public interest or legitimate interests of the controller. The controller must cease such processing unless it demonstrates compelling legitimate grounds for the processing that override the interests, rights and freedoms of the relevant data subject or requires the data in order to establish, exercise or defend legal rights.
- **Right to restrict processing**
  Data subjects have the right to restrict the processing of personal data, which means that the data may only be held by the controller, and may only be used for limited purposes if: (i) the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); (ii) the processing is unlawful and the data subject requests restriction (as opposed to exercising the right to erasure); (iii) the controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights; or (iv) verification of overriding grounds is pending, in the context of an erasure request.
- **Right to data portability**
  Data subjects have a right to receive a copy of their personal data in a commonly used machine-readable format, and transfer their personal data from one controller to another or have the data transmitted directly between controllers.
- **Right to withdraw consent**
  A data subject has the right to withdraw their consent at any time and must be informed of this right prior to giving consent. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. It must be as easy to withdraw consent as it is to give it.

- **Right to object to direct marketing**
  Data subjects have the right to object to the processing of their personal data for the purposes of direct marketing, including profiling and to opt out of direct marketing communications.
- **Right protecting against solely automated decision-making and profiling**
  Data subjects have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects that concern (or similarly significantly affect) them. This right is restricted where the solely automated decision: (i) is necessary for entering into, or the performance of, a contract between the data subject and controller; (ii) is authorised by EU or Member State law to which the controller is subject (and which contains suitable measures to safeguard the data subject's rights); or (iii) is based on the data subject's explicit consent.
- **Right to complain to the relevant data protection authority(ies)**
  Data subjects have the right to lodge complaints concerning the processing of their personal data with the DPC if the data subjects live in Ireland or the alleged infringement occurred in Ireland.
- **Right to basic information**
  Data subjects must be furnished with certain information and be informed of all their rights in respect of their personal data. Such information includes the identity of the controller, the reasons for processing their personal data and the time period for which the personal data will be held. Such rights include the right to object to processing, the right of access, the right to withdraw consent and the right to lodge a complaint with the DPC. The provision of this information to the data subject is necessary to ensure the fair and transparent processing of personal data.
- **Right to compensation**
  Data subjects who have suffered (material or non-material) damage as a result of the unlawful processing of their personal data have the right to receive compensation from the controller and/or processor for the harm suffered. The recent Circuit Court decision of *Kaminski v. Ballymaguire Foods Limited [2023] IECC* 5 provides clarity on the courts assessment for non-material damages due to breaches of the GDPR, indicating that compensation for non-material damage is likely to be very modest in future cases of this nature.

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

Where a data subject considers that their rights under the GDPR have been infringed, they have the right to mandate not-for-profit organisations that: (i) have been properly constituted in accordance with the laws of Ireland; (ii) have statutory objectives that are in the public interest; and (iii) are active in the field of the protection of data subjects' rights and freedoms. The mandated organisations may lodge a complaint with the DPC and/or seek a judicial remedy on behalf of the data subject.

This right is reiterated in section 117(7) of the DPA 2018, which allows for a data protection action to be brought on behalf of a data subject by a not-for-profit body, organisation or association on the instruction of the data subject.

Further, the Collective Interests of Consumers Bill 2022 will transpose Directive (EU) 2020/1828 into Irish law. The Directive provides for "Qualifying Entities" to bring representative actions, that is class actions, on behalf of consumers, including, explicitly, class actions based on the infringements of rights under the GDPR.

6 Children's Personal Data

6.1 What additional obligations apply to the processing of children's personal data?

Article 8(1) of the GDPR provides that where information society services are offered directly to a child under the age of 16, and the lawful basis of processing their personal data is consent, such consent must be obtained from or authorised by the individual with parental responsibility over the child. The controller must make reasonable efforts to verify that consent has been given, or authorised, by the holder of parental responsibility in light of available technology.

Section 29 of the DPA 2018 confirms that references to a "child" in the GDPR shall be taken to refer to a person under the age of 18. The DPA 2018 creates an offence for a company or corporate body to process the personal data of a child for the purposes of direct marketing, profiling or micro-targeting. At the time of writing, this section has not been commenced.

The DSA came into effect in November 2022. The General Scheme of the (Irish) Digital Services Bill was published in February 2023 and will give full effect to the DSA. The DSA prohibits targeted advertising aimed at children and requires service providers to carry out a risk assessment of the risk that their platform may pose to children.

The protection of children's rights continues to be a priority for the DPC and remains one of the five strategic goals of its 2022–2027 Regulatory Strategy. In December 2021, the DPC published "Fundamentals" on the processing of children's personal data, which introduced child-specific data protection interpretative principles and recommended measures to enhance the level of protection afforded to children. In May 2023, the DPC published three short guides for children aged 13 and over on their data protection rights.

Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in a clear and plain language that the child can easily understand.

7 Registration Formalities and Prior Approval

7.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

There are no registration requirements for controllers or processors in Ireland. Under section 88 of the DPA 2018, all organisations that have appointed a Data Protection Officer ("**DPO**") pursuant to the GDPR, are required to notify the contact details to the DPC, which holds a register of DPOs. A controller is obliged to publish the contact details of the DPO so that it is easily accessible to data subjects.

7.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

This is not a requirement in Ireland.

7.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

This is not a requirement in Ireland.

7.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

Only registration of the DPO is required.

7.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

The entity's name, address, email, telephone number and URL, and the DPO's name, email address and telephone number.

7.6 What are the sanctions for failure to register/notify where required?

No such sanctions apply.

7.7 What is the fee per registration/notification (if applicable)?

There is no applicable fee.

7.8 How frequently must registrations/notifications be renewed (if applicable)?

Notification of change of a DPO should be notified to the DPC without delay.

7.9 Is any prior approval required from the data protection regulator?

Where a controller determines, by way of Data Protection Impact Assessment ("**DPIA**") that the intended processing would result in a high risk to the data protection rights of individuals, in the absence of mitigation measures, they must consult with the DPC.

7.10 Can the registration/notification be completed online?

Registration of a DPO can be undertaken through the DPC's online form.

7.11 Is there a publicly available list of completed registrations/notifications?

There is no publicly available list of completed DPO registrations.

7.12 How long does a typical registration/notification process take?

The registration of the DPO can be completed in a matter of minutes on the DPC website.

8 Appointment of a Data Protection Officer

8.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

A DPO must be appointed in the following circumstances: (i) when processing is conducted by a public authority or body, excluding courts in their judicial role; (ii) when the primary activities of the controller or processor involve processing operations that, due to their nature, extent and/or purposes, necessitate regular and systematic monitoring of a large number of data subjects; or (iii) when the primary activities of the controller or processor involve processing on a large scale of sensitive categories of data and personal data concerning criminal convictions and offences. Apart from these scenarios, associations and other bodies representing groups of controllers or processors may choose (or be legally required under the laws of their Member State) to appoint a DPO. Additionally, a group of companies may opt to designate a single DPO.

Under Section 26 of the DPA 2018, the appointment of a DPO can be considered an appropriate and specific measure needed to protect the fundamental rights and freedoms of data subjects in certain cases.

Under Section 34 of the DPA 2018, the relevant Minister may establish regulations mandating controllers, processors, associations, or other bodies representing categories of controllers or processors to appoint a DPO. At the time of writing, no such regulations have been enacted.

8.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

The penalty for failure to appoint a DPO, where one should have been appointed, is an administrative fine of up to EUR 10 million, or in the case of an undertaking, up to 2% of total worldwide annual turnover of the preceding financial year. Further corrective powers of the DPC may be invoked for breaches of the GDPR, e.g. the issuance of warnings and reprimands, orders to bring processing into compliance, orders to cease processing and the imposition of a ban on processing.

8.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

The designated DPO must not face dismissal or penalties from a controller or processor for carrying out their duties. They are required to function autonomously and should report directly to the highest management level of the controller or processor.

8.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

A group of undertakings may appoint a single DPO, provided that they are easily accessible for each establishment.

8.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The DPO must be designated on the basis of professional qualities and in particular expert knowledge of data protection law and practices and the ability to fulfil tasks set out in the GDPR, these being: (i) informing and advising the controller or processor and the employees who carry out processing of their obligations under the GDPR and Irish data protection law; (ii) monitoring compliance with the GDPR and Irish data protection law; (iii) providing advice where requested in regard to the DPIA and monitoring its performance; (iv) cooperating with the DPC as supervisory authority; and (v) acting as the contact point for the DPC as supervisory authority on issues relating to processing.

8.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

The DPO is required to: (i) provide information and guidance to the controller or processor and the employees who carry out processing regarding their responsibilities under the GDPR and Irish data protection law; (ii) oversee adherence to the GDPR and Irish data protection law; (iii) offer advice upon request concerning DPIAs and supervise their implementation; (iv) collaborate with the DPC as the supervisory authority; and (v) act as a the contact point for the DPC as supervisory authority on issues relating to processing.

8.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

The appointment of the designated DPO and their contact details must be notified to the DPC.

8.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

Where a controller appoints a DPO, it must publish the contact details of the DPO. This, however, does not necessarily mean that the DPO needs to be named in public-facing documents, as the contact details may be anonymised, e.g. an anonymised email address such as dpo@iclgbyrnewallace.ie.

The transparency requirements of the GDPR require that the contact details of the DPO be furnished to data subjects at the time when personal data is collected from them.

9 Appointment of Processors

9.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes, the business is required to enter into a Data Processing Agreement with the processor which sets out: (i) the subject matter for processing; (ii) the duration of processing; (iii) the nature and purpose of processing; (iv) the types of personal data and categories of data subjects; and (v) the obligations and rights of the controller.

9.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The processor must be engaged through a binding written agreement. This agreement should include terms that specify that the processor: (i) only acts on the documented instructions provided by the controller; (ii) enforces confidentiality obligations on all employees involved; (iii) ensures the security of the personal data it processes; (iv) adheres to the rules regarding the appointment of sub-processors; (v) implements measures to assist the controller in upholding the rights of data subjects; (vi) assists the controller in obtaining approval from the relevant data protection authority; (vii) either returns or securely destroys the personal data at the termination of the relationship (unless otherwise obligated by EU or Member State law); and (viii) furnishes the controller with all necessary information to demonstrate compliance with the GDPR.

10 Marketing

10.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

The ePrivacy Regulations, which transpose the ePrivacy Directive into Irish law, outline specific rules with regard to the use of marketing communications. Consent is required in respect of electronic direct marketing for new customers. Consent is not required in respect of electronic direct marketing for existing customers, where certain conditions are satisfied.

10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

Although the specific rules and requirements for consent in the ePrivacy Regulations generally apply to natural persons, in relation to direct marketing by telephone calls, there is no distinction in the ePrivacy Regulations between unsolicited telephone communications to individuals and those to companies and all other persons other than natural persons. The regulation of such direct marketing calls differs depending on whether they are made to landlines or to mobile phones.

Unsolicited direct marketing by fax and call by automated calling machine to companies and all persons other than natural persons are regulated on an opt-out basis, that is, they are permitted until the intended recipient notifies the sender that it does not consent.

10.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

Unsolicited marketing calls to landlines (but not mobiles) are

permitted until the recipient opts out by informing the caller of their withdrawal of consent. Similarly, unsolicited fax marketing is permissible until the recipient opts out by informing the sender of their withdrawal of consent. Direct marketing via postal mail is not covered by the ePrivacy Regulations, but it remains subject to the requirements outlined in the GDPR and the DPA 2018.

10.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?

The ePrivacy Regulations apply to entities sending direct marketing communications to recipients in Ireland. Direct marketers operating from abroad, including those sending marketing from outside the EU, are subject to the laws of their respective jurisdictions. It is important to note that the GDPR has significant extraterritorial reach, providing rights and safeguards to data subjects within the EU, irrespective of where the processing occurs.

10.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

There is evidence of the DPC enforcing data protection and direct marketing laws across all sectors. Please also see our answers to questions 11.3 and 19.1.

10.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Data sets, such as marketing lists, are captured by the broad definition of processing. Therefore, a controller must comply with all of the legal obligations applicable to the processing of personal data under the GDPR, including the fundamental principles as outlined above. A purchaser of a marketing list will need to verify the data's usability, i.e. ensuring its lawful collection and subsequent use. This would include reviewing the vendor's record of processing activities to ensure the vendor has complied with all legal requirements, such as obtaining valid consent and conducting a legitimate interest assessment.

10.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

The DPC lacks the authority to impose fines for violations of the ePrivacy Regulations. However, it possesses other enforcement capabilities, such as conducting investigations based on complaints or its own initiative, issuing enforcement notices that mandate compliance with specific requirements, and the power to disclose the identities of parties responsible for breaches along with details of the infringements.

Breaches of the ePrivacy Regulations may lead to criminal prosecution through the Irish courts. Upon summary conviction, the sender of a marketing communication may face a fine not exceeding EUR 5,000 per offence, while on indictment, a fine not exceeding EUR 250,000 per offence. Notably, if a marketer sends 100 emails, each email can be held to be a separate offence.

11 Cookies

11.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

The ePrivacy Regulations prohibit the use of cookies or other tracking technologies that are not strictly necessary unless the user has given explicit consent to that use. The standard of consent is that set out in the GDPR. Consent for the placement of non-essential cookies is not valid if it was either bundled or obtained by way of pre-checked boxes that users must deselect. Controllers must ensure that opt-in consent is obtained for each purpose for which cookies are set and consent must be as easy to withdraw as it was to provide in the first place for the user.

11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

Consent for cookies or other tracking technologies is required where the cookies or tracking technologies are non-essential. As a result, third-party, performance, targeting cookies, etc. will require opt-in consent that can be as easily withdrawn by the user as it was given.

11.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

There is evidence of the DPC enforcing the ePrivacy Regulations across all sectors. In 2023, the DPC prosecuted four companies for the sending of unsolicited marketing communications without consent to individuals. The DPC concluded 237 electronic direct-marketing investigations in 2023.

11.4 What are the maximum penalties for breaches of applicable cookie restrictions?

The DPC is not empowered by law to issue fines for breach of the ePrivacy Regulations and it is not an offence in Ireland to violate the legal requirements for cookies and other tracking technologies. However, the DPC does have other enforcement powers, e.g. complaint-based and/or own volition investigations of alleged contraventions, enforcement notices that oblige recipients to comply with specific requirements, and the power to publish the names of parties responsible for and details of ePrivacy breaches. Please also see our answer to question 10.7.

12 Restrictions on International Data Transfers

12.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Transfers of personal data from Ireland to non-EEA or "third" countries are governed by Chapter V of the GDPR. Such transfers are permitted either where there is a European Commission adequacy decision in place or, alternatively, where appropriate safeguards are implemented, such as standard contractual clauses ("**SCCs**") or binding corporate rules ("**BCRs**"), under

Article 46 of the GDPR. Derogations may also apply in limited circumstances under Article 49 of the GDPR, e.g. where a data subject explicitly consents.

In June 2021, the European Commission approved four separate modular sets of SCCs and the appropriate module to be used will depend on the data protection role of the data exporter and data importer. Where SCCs are used, they should comply with the EDPB recommendations (Recommendations 01/2020) on measures to support the implementation of the decision in C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems* ("***Schrems II***"). In particular, the exporter must carry out a transfer risk assessment and also identify and implement supplementary measures to ensure an "essentially equivalent" level of protection applies to the personal data throughout the transfer to the third country.

12.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

Absent an adequacy decision, businesses may make transfers to non-EEA jurisdictions by putting in place appropriate safeguards, such as SCCs or BCRs. Derogations may also apply in limited circumstances under Article 49 of the GDPR, e.g. where a data subject explicitly consents to the transfer**.**

Transfer of personal data to the US is also possible if the data importer has signed up to the EU–US Data Privacy Framework, which has been designed by the US Department of Commerce in consultation with the European Commission to provide businesses in the EU and the US with a mechanism to comply with data protection requirements when transferring personal data from the EU to participating US companies and government agencies.

12.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

Approval of the DPC *per se* is not required for transfers to non-EEA jurisdictions. However, BCRs require approval of the relevant supervisory authority. There are, at the time of writing, 21 such approved BCRs for which the DPC is the lead supervisory authority ("**LSA**"). SCCs are those adopted by the European Commission, with the Commission having approved four separate modular sets of SCCs in June 2021.

As noted above, transfers to non-EEA or "third" countries are permitted where there is a European Commission adequacy decision in place or alternatively where appropriate safeguards are implemented, such as SCCS or BCRs.

12.4 Do transfers of personal data to other jurisdictions require a transfer impact assessment? If conducting a transfer impact assessment is only mandatory in some circumstances, please identify those circumstances.

A Transfer Impact Assessment ("**TIA**") is only required when transferring personal data to a third country outside the EEA that is not covered by a European Commission adequacy decision. Conducting a TIA is a legal obligation for all EU-based data exporters who intend to carry out a restricted transfer by relying on one of the transfer tools in Article 46 of the GDPR.

12.5 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?

Although the DPC has not issued any official guidance following *Schrems II*, it has noted on its website that *Schrems II* will have an impact on BCRs, in that, before making transfers within a corporate group from members within the EEA to members in third countries, and taking into account the specific circumstances of the transfer, an assessment must be carried out on the level of protection and possible need for supplementary measures or suspension of the transfer.

The EDPB has issued Recommendations 01/2020 on supplementary protections to be implemented where appropriate, in respect of transfers made under SCCs, in light of the *Schrems II* decision. These Recommendations are designed to assist data exporters with the task of assessing the laws of third countries and identifying appropriate measures to implement where the level of protection afforded to personal data is not essentially equivalent to that within the EEA. Such protections include technical measures (e.g. pseudonymising personal data or encrypting it while in transit), contractual measures (e.g. certification by a data importer that it has not created any "back doors" that could be used to access the personal data or contractual provision for a "warrant canary" method) and organisational measures (e.g. ensuring adequate internal policies that contain clear allocation of responsibilities for data transfers or regular publication of transparency reports).

12.6 What guidance (if any) has/have the data protection authority(ies) issued in relation to the use of standard contractual/model clauses as a mechanism for international data transfers?

The DPC has not provided any specific guidance on this point and merely guides users to the European Commission's "Questions and Answers" on the use of the SCCs on their website.

13 Whistle-blower Hotlines

13.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

The Protected Disclosures Act 2014, as amended (the "**2014 Act**"), transcribes EU Directive 2019/1937 on the protection of persons who report breaches of Union law (commonly known as "**whistleblowing**"). The 2014 Act sets out detailed requirements and obligations in relation to internal whistleblowing reporting channels for employers with over 50 employees. The 2014 Act details the types of wrongdoing to which it applies, the categories of persons who will be protected if they make a report of a wrongdoing, and the protections applying to the reporting person, including protection of identity and protection from penalisation. The 2014 Act also sets out the process for accepting, acknowledging and following up on reports of wrongdoing from reporting persons. Processing of such personal data will mainly be carried out in order to comply with the legal obligations set out in the 2014 Act.

The 2014 Act permits limitations on certain data protection rights and obligations provided for in Articles 12 to 22 and Article 34 of the GDPR, where necessary and proportionate. This is done to, among other objectives, prevent and address efforts to obstruct reporting or impede the follow-up on reports, or to uncover the identity of whistle-blowers.

Although the 2014 Act establishes minimum requirements, it does not restrict corporate whistleblowing processes from exceeding its provisions. Companies may accept reports on a broader range of issues and from a wider array of individuals, or may implement processes for employers with fewer than the specified number of employees. Processing of personal data in such cases should be conducted on a lawful basis as per Article 6 of the GDPR, which may include the legitimate interests of the employer.

13.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

According to the 2014 Act, employers are not compelled to receive and act upon anonymous reports; nonetheless, they retain the option to do so if they so choose. In the event that an anonymous report is accepted, it must be handled in a manner consistent with any other report made under the 2014 Act, to the fullest extent possible considering its anonymous nature. Employers have the discretion to stipulate in their relevant internal policy whether they will accept anonymous reports.

14 CCTV

14.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

Where a controller determines by way of a DPIA that the intended processing would result in a high risk to the data protection rights of individuals then, in the absence of mitigation measures, they must consult with the DPC. In addition, where the monitoring of publicly accessible areas (whether by CCTV or otherwise) is being undertaken on a large scale, the recitals to the GDPR state that a DPIA is required.

Beyond this, no specific prior registration/notification or prior approval is required for CCTV use.

The DPC has issued guidance on the use of CCTV, which includes a "CCTV Checklist", the questions on which should be considered prior to installing a CCTV system. These questions include:

(i) Do you have a clearly defined purpose for installing CCTV?
(ii) What is the legal basis for your use of CCTV?
(iii) Can you demonstrate that CCTV is necessary to achieve your goal?
(iv) If your CCTV system is to be used for purposes other than security, are you able to demonstrate that those other uses are proportionate?

In addition to considering the CCTV Checklist, best practice recommends that a controller put in place a CCTV policy that is compliant with DPC guidelines. Controllers should also ensure that data subjects are informed of their rights in respect of their personal data processed through the use of CCTV and that the CCTV policy is published on the controller's website so that members of the public that visit the controller's premises are aware of the policy in advance.

14.2 Are there limits on the purposes for which CCTV data may be used?

Although the DPC guidance does not provide any limits on the purposes for which CCTV data may be used, it does advise that unless CCTV is used proportionately, it can give rise to legitimate concerns of unreasonable and unlawful intrusion into the data protection and privacy rights of individuals and monitoring or surveillance may be taking place. The DPC guidance further states that a controller must be able to justify the use of a CCTV system as both necessary to achieve their given purposes and proportionate in its impact upon those who will be recorded.

The following questions in respect of the purpose of processing form part of the "CCTV Checklist":

(i) Do you have a clearly defined purpose for installing CCTV?
(ii) What are you trying to observe taking place?
(iii) Is the CCTV system to be used for security purposes only? If not, can you justify the other purposes?
(iv) Will the use of the personal data collected by the CCTV be limited to that original purpose?

15 Employee Monitoring

15.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Employee monitoring is permitted by employers, provided that there is a lawful basis to do so. The type of monitoring permitted will depend on the nature and circumstances of the employment, and extent of monitoring being carried out. Employees must be informed that the monitoring is being carried out, and the purpose for which it is being carried out.

15.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

While consent is one such lawful basis, it is seldom used in employment contexts, due to concerns regarding the imbalance of power between employers and employees, which could affect the validity of consent. According to the EDPB Guidelines 05/2020 on consent under the GDPR, relying on employee consent for most data processing at work is discouraged.

Instead, employers typically rely on the lawful basis of legitimate interest to justify employee monitoring. However, this requires that the monitoring is proportionate, necessary to achieve the legitimate interest, and does not override the interests or fundamental rights and freedoms of the employee. Notice of monitoring should be provided, usually through a data protection policy or other relevant employment policy, to ensure transparency and compliance with data protection regulations.

15.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

There is no legal requirement to notify or consult with works councils or trade unions; however, such consultation may take place as part of best practice.

15.4 Are employers entitled to process information on an employee's attendance in office (e.g., to monitor compliance with any internal return-to-office policies)?

The DPC has not provided any specific guidance on employers monitoring their employees' attendance in the context of any internal return-to-office policies. However, the DPC has issued extensive guidance on the use of CCTV in the workplace and employee vehicle tracking. The DPC also recognises that employers have a legitimate interest in protecting their business, reputation, resources and equipment. To achieve this, they may decide to monitor their employees' use of the internet, email and telephone. The DPC warns, however, that any limitation of employees' right to privacy should be proportionate to the likely damage to the employer's legitimate interests. An acceptable-use policy should be adopted reflecting this balance and employees should be aware of the scope and purposes of the monitoring specified. In the absence of a clear acceptable-use policy, employees may be assumed to have a reasonable expectation of privacy in the workplace.

16 Data Security and Data Breach

16.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Yes. Controllers and processors are obliged to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk arising from processing activities. Neither the GDPR, nor the DPA 2018, stipulate any specific security measures. The GDPR lists certain considerations that should be taken into account, such as the costs of implementation and the nature, scope, context and purposes of processing. The DPC has issued Guidance for Controllers on Data Security dated February 2020.

The ePrivacy Regulations impose certain security obligations on undertakings providing a publically available electronic communications network or service. Security measures must at least ensure that the personal data can be accessed only by authorised personnel for legally authorised purposes, protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure, and ensure the implementation of a security policy with respect to the processing of personal data.

16.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

A controller is responsible for reporting a personal data breach without undue delay (and in any case within 72 hours of first becoming aware of the breach) to the relevant data protection authority, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject(s). A controller must document any personal data breach.

The notification must include, at least, the following information: (i) the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; (ii) the name and contact details of the DPO or other contact point; (iii) the likely consequences of the personal data breach; and (iv) the measures taken or proposed to be taken by the controller to address the breach, including, where appropriate, measures to mitigate its possible adverse effects. A processor must also notify any data breach to their controller without undue delay.

16.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Controllers are obliged to notify affected data subjects of the personal data breach where the breach is "likely to result in a high risk to the rights and freedoms of the natural person". No such reporting obligation to the data subject arises where: (i) the controller has implemented technical and organisational measures that render the personal data unintelligible to third parties, e.g. encryption; (ii) the controller has taken subsequent measures to ensure that the high risk to the data subject's rights do not materialise; or (iii) it would involve disproportionate effort.

The notification must describe in clear and plain language the nature of the breach and at the least: (i) the name and contact details of the DPO or other contact point; (ii) the likely consequences of the personal data breach; and (iii) the measures taken or proposed to be taken by the controller to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

16.4 What are the maximum penalties for personal data security breaches?

Regulatory fines for breaches of data protection law can be up to the greater of EUR 20 million or 4% of global annual turnover of the relevant organisation for the preceding financial year, depending on the nature of the infringement. Other sanctions include a temporary or permanent ban on the processing of personal data, a reprimand or withdrawal of certification.

The DPC has various and wide powers, in addition to or as an alternative to a financial penalty, e.g. powers to issue a warning, impose a reprimand, issue various orders such as order a controller to comply with the data subject's request(s), to bring processing operations into compliance or to impose a ban on processing.

The DPA 2018 imposes a maximum fine of up to EUR 1 million on public authorities, or bodies that do not act as an undertaking within the meaning of the Irish Competition Act 2002.

The maximum criminal penalty for summary offences under the DPA 2018 is EUR 5,000 and/or 12 months' imprisonment. Indictable offences carry a maximum penalty of EUR 250,000 and/or five years' imprisonment.

The DPC does not have the power to impose regulatory fines pursuant to the ePrivacy Regulations. However, it has the power to prosecute offences under these regulations. A summary offence carries a maximum fine of EUR 5,000. Indictable offences carry a maximum fine of EUR 250,000, depending on the nature of the offence being prosecuted.

17 Enforcement and Sanctions

17.1 Describe the enforcement powers of the data protection authority(ies).

- **Investigative Powers:** The DPC possesses broad investigatory (and enforcement) powers, including: (i) search and seizure powers; (ii) powers to issue information and enforcement notices for which failure to comply is an offence; and (iii) the right to apply to the Irish High Court for the suspension or restriction of processing of data, where it is considered that there is an urgent need to act. The DPC also has the power to prosecute offences under the Act and the ePrivacy Regulations.
- **Corrective Powers:** The DPC possesses broad corrective powers including: (i) powers to issue warnings or reprimands for non-compliance; (ii) to order the controller to disclose a personal data breach to the data subject; (iii) to impose a permanent or temporary ban on processing; and (iv) to impose an administrative fine.
- **Authorisation and Advisory Powers:** The DPC possesses broad authorisation and advisory powers, including: (i) advise controllers; (ii) issue opinions to the government or other institutions; (iii) authorise processing; (iv) issue opinions and draft codes of conduct; (v) accredit certification bodies; (vi) issue certifications; and (vii) adopt and authorise SCCs and approve BCRs.
- **Imposition of administrative fines for infringements of specified GDPR provisions:** The DPC may impose regulatory fines for breaches of data protection law of up to EUR 20 million or 4% of global annual turnover of the relevant organisation for the preceding financial year, whichever is the greater, depending on the nature of the infringement.
- **Non-compliance with a data protection authority:** Failure to comply with the DPC (or any supervisory authority under the GDPR) under Article 31 of the GDPR, may give rise to a fine under Article 83(4) of the GDPR of the higher of EUR 10 million or 2% of global annual turnover of the relevant organisation for the preceding financial year, whichever is the greater.

17.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

Section 134 of the DPA 2018 permits the DPC, where it identifies an urgent need to protect data subjects' rights and freedoms under a relevant act or statutory instrument, to make an application to the High Court (which may be *ex parte* under Section 134(4) of the DPA 2018) for an order to suspend, restrict or prohibit the processing of personal data.

17.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

The DPC has acquired a reputation as an active enforcement body by virtue of the GDPR's "one-stop-shop mechanism" ("**OSS**"), which allows organisations that are engaged in cross-border EU data processing to deal with a single LSA for their data protection compliance obligations.

Of note in 2023 was the conclusion of the DPC's investigation into the lawfulness of Meta's transfers of personal data from the EU to the US, and the DPC's investigation in relation to TikTok and child users. Final decisions in these cases were adopted in May (Meta), and September (TikTok) 2023, imposing fines of EUR 1.2 billion and EUR 345 million, respectively. A feature of this regulation has seen the companies concerned bring multiple concurrent sets of legal proceedings before the Irish High Court and the European Courts challenging the outcome of DPC inquiries and the process by which they were concluded.

17.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

The OSS facilitates the regulation of entities established in the EU that engage in cross-border processing. It comes into effect when an entity conducts cross-border processing and has multiple establishments within the EU. The LSA for such an entity is the supervisory authority of the Member State where the entity's main establishment is located. The LSA assumes primary responsibility for overseeing the entity's processing activities and serves as the main point of contact for cross-border processing matters in most instances. The OSS operates within the framework of the GDPR's cooperation and consistency mechanism.

In 2023, the DPC received 156 valid cross border complaints, relating to companies for whom the DPC is the LSA. By year end, the DPC had concluded 279 cross border complaints. During this period, a further 13 complaints were lodged with the DPC where another supervisory authority was identified as the LSA.

The DPC serves as the lead LSA for numerous multinational companies across the EU that have their European headquarters situated in Ireland. Notably, the DPC has taken on high-profile inquiries and enforcement actions, including the Meta and TikTok decisions, as well as decisions against companies such as Airbnb, Twitter and Groupon. It is important to note that the rules governing the LSA and the OSS do not apply to processing carried out by public authorities or private bodies in the public interest.

18 E-discovery/Disclosure to Foreign Law Enforcement Agencies

18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

In the first instance, a business will typically check if the request is legitimate. A business must be satisfied that any processing of personal data pursuant to a request from a foreign enforcement agency is compliant with the GDPR, there must be a lawful basis for processing pursuant to Article 6, and in the case of special-category data, one of the conditions in Article 9 must also be satisfied. Where requests for disclosure have been made by foreign law enforcement agencies, this data may constitute personal data relating to criminal convictions and offences. If this is the case, the business must also ensure compliance with Article 10 of the GDPR, and section 55 of the DPA 2018.

If processing is conducted for purposes other than those for which the data was collected, it is lawful to the extent that it is necessary and proportionate for:

- preventing a threat to national security, defence or public security;

- preventing, detecting, investigating or prosecuting criminal offences; and
- providing or obtaining legal advice in the context of legal proceedings or establishing, exercising and defending legal rights.

Given the risk and time involved in this legal assessment, businesses often direct the requestor to the mutual legal assistance process outlined in the Criminal Justice (Mutual Assistance) Act 2008. The Minister for Justice serves as the Irish Central Authority for Mutual Assistance, responsible for coordinating correspondence between domestic and foreign authorities for both incoming and outgoing requests, as well as performing administrative functions related to coordinating requests.

18.2 What guidance has/have the data protection authority(ies) issued on disclosure of personal data to foreign law enforcement or governmental bodies?

The DPC has issued general guidance on the legal bases for processing personal data but has not issued formal guidance addressing disclosure to foreign law enforcement agencies at the time of writing.

19 Trends and Developments

19.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

The DPC successfully addressed 89 statutory inquiries during the year, including 51 cross-border inquiries. Several large-scale inquiries were also concluded, with administrative fines imposed by the DPC exceeding EUR 1.5 billion, which accounted for 87% of the fines in the entirety of the EU, EEA and UK. Since the enactment of the GDPR, the DPC has issued sanctions for infringements of the GDPR totalling EUR 2.86 billion. Further, the DPC issued 19 finalised decisions, along with multiple reprimands and compliance orders being imposed. Notable cases include:

- Meta (Facebook): The DPC announced the conclusion of its inquiry into Meta Platforms Ireland Limited, concerning data transfers from the EU to the US. The decision imposed a fine of EUR 1.2 billion on Meta Ireland, in addition to an order to bring its processing operations into compliance.
- TikTok: The DPC issued its final decision in its inquiry into TikTok Technology Limited. The inquiry examined the processing of personal data relating to children by TikTok. The Decision ordered TikTok to bring its processing into compliance and imposed fines totalling EUR 345 million.
- Bank of Ireland: This inquiry was in relation to a series of data breaches on the Bank of Ireland 365 app and the failure of the bank to implement appropriate technical and organisational measures to protect the personal data of its customers. The DPC exercised its corrective powers, which included a reprimand, a fine of EUR 750,000 and an order to bring processing into compliance.

A total of 237 electronic direct marketing investigations were concluded in 2023, and the DPC prosecuted four companies for the sending of unsolicited marketing communications without consent. The Court returned convictions on all charges and it imposed fines totalling EUR 2,000.

The protection of children's rights continues to be a priority for the DPC and remains one of the five strategic goals of its 2022–2027 Regulatory Strategy. Following publication of the DPC's Fundamentals to a Child-Oriented Approach to Data Processing in December 2021, in May 2023, the DPC published three short guides for children aged 13 and over on their data protection rights.

19.2 What "hot topics" are currently a focus for the data protection regulator?

Artificial intelligence ("**AI**") will continue to be a focal point for the DPC in 2024 and beyond. The EU Artificial Intelligence Act ("**AI Act**") will enter into force this year on a graduated basis, with all provisions to be fully implemented by 2026. The AI Act requires Member States to provide for supervision and enforcement at national level. However, at the time of writing, there is no indication as to what entity will be responsible for regulating AI in Ireland. Dale Sunderland, the Deputy Data Protection Commissioner of Ireland, has confirmed that there has already been "extensive engagement" with the DPC by leading US tech firms based in Ireland, to ensure that their AI products do not fall foul of the GDPR. As such, it remains to be seen whether the regulation of AI will fall under the remit of an existing body, such as the DPC, or whether the Irish government will create a new bespoke entity. Regardless, the DPC is expected to play a key role in ensuring organisations maintain data protection compliance when the AI Act comes into force.

Online safety and the protection of children's personal data is expected to remain a key priority for the DPC, in line with the five strategic goals of its 2022–2027 Regulatory Strategy. In September 2023, the DPC issued a final decision in its inquiry into TikTok Technology Limited, concerning the processing of personal data relating to children. The DPC focused on several areas of non-compliance in its decision, namely: (i) public-by-default settings; (ii) settings associated with the "family pairing" feature; (iii) transparency information provided to child users; and (iv) issues with age verification. The DPC ordered TikTok to bring its processing into compliance and imposed administrative fines totalling EUR 345 million. The decision is currently under appeal by TikTok.

Data subject access requests ("**DSARs**") have played a prominent role in the DPC's decisions over the last year, and this trend is expected to continue. DSARs accounted for 39% of the top five complaints received by the DPC under the GDPR in 2023. In February 2024, the EDPB formally launched its third Coordinated Enforcement Framework ("**CEF**"). The focus of this year's action is on DSARs, as set out in Article 15 of the GDPR. The CEF seeks to streamline enforcement and cooperation amongst data protection authorities in Europe, with previous years focusing on the public sector's use of cloud services and DPOs. This year, 31 participating data protection authorities will circulate fact-finding questionnaires to organisations in their territory, with the aim of identifying the need for formal investigations and launching such investigations where appropriate. At the conclusion of the CEF, results will be aggregated to offer a pan-European overview and to facilitate targeted follow-up at the EU level. The EDPB will publish a report of these outcomes once the actions are concluded. On 19 March 2024, the DPC announced that it will be participating in this year's CEF.

Victor Timon is Head of the Technology Group at ByrneWallace LLP. He has nearly 40 years' experience in the technology industry, having worked both as an in-house Counsel in global technology companies and as a Partner in a number of law firms in Dublin and London.
Victor's practice has evolved from more traditional IT projects (such as software licensing, equipment procurement, outsourcing, etc.) into cloud computing, e-commerce, digital communications, AI, block chain, NFTs, cyber security and social media. He is also an expert in intellectual property and data protection. He regularly speaks at in-people conferences and webinars and publishes articles on these topics. He has also authored the Ireland chapters of a number of international publications on AI, Digital Business and Cybersecurity. Victor is on the Advisory Board of Digital Business Ireland, the representative body for the digital commerce sector, and chairs its Policy Committee.

ByrneWallace LLP
88 Harcourt Street
Dublin 2
Ireland

Tel: +353 1 691 5000
Email: vtimon@byrnewallace.com
LinkedIn: www.linkedin.com/in/victortimontechprivacylawyer

Zelda Deasy is a Partner in the ByrneWallace LLP Corporate Department specialising in data protection and commercial contracts. She has over 20 years' experience in advising clients in the telecoms, technology, construction, energy, transport, life sciences, healthcare, financial services and FMCG sectors. Zelda's clients include companies at all stages of development from start-ups and entrepreneurs to SMEs and scaling companies to large domestic and multi-national organisations and public bodies. Zelda advises both private-sector organisations and public bodies on all data protection matters, including drafting, reviewing and negotiating data transfer/data sharing agreements, data processing agreements, online terms and conditions, privacy/cookies policies and data protection policies.

ByrneWallace LLP
88 Harcourt Street
Dublin 2
Ireland

Tel: +353 1 691 5000
Email: zdeasy@byrnewallace.com
LinkedIn: www.linkedin.com/in/zeldadeasy

Seán O'Donnell is a Partner in ByrneWallace LLP and leads the firm's cross-departmental Privacy and Data Protection Team, overseeing and advising on all aspects of data protection law. Seán's background as a dispute resolution and regulatory lawyer is invaluable in engagements with the regulator, the Data Protection Commission. He advises clients on risk and mitigation of risk having regard to the Data Protection Regulatory Framework to include the e-Privacy Regulations. Seán also advises on the application of the Law Enforcement Directive.
Seán has been instrumental in driving a cultural change amongst various clients to successfully embed compliance with GDPR within their organisations, having participated in several steering groups responsible for ensuring a GDPR-compliant framework is implemented and that such a framework can be adhered to in the practical undertaking of operations.

ByrneWallace LLP
88 Harcourt Street
Dublin 2
Ireland

Tel: +353 1 691 5000
Email: sodonnell@byrnewallace.com
LinkedIn: www.linkedin.com/in/sean-o-donnell-206b2835

Mark Condy is a Solicitor and part of the cross-departmental Privacy and Data Protection Team. Having previously worked as part of the in-house legal team for a large international pharmaceutical company and trained in a corporate law firm, Mark recently joined ByrneWallace to add to the growing data protection practice. Mark advises various public and private clients across a range of sectors, from established health providers to new tech start-ups, on data protection and privacy-related issues.

ByrneWallace LLP
88 Harcourt Street
Dublin 2
Ireland

Tel: +353 1 691 5000
Email: mcondy@byrnewallace.com
LinkedIn: www.linkedin.com/in/mark-condy

ByrneWallace LLP is one of Ireland's largest full-service law firms. A forward-thinking Irish law firm, it focuses on securing the best possible outcomes for its clients and is dedicated to the protection and promotion of its clients' interests through the provision of expert legal services. This expertise is borne out of close to half a century of delivering high professional standards and developing some of the most talented lawyers in Ireland.
In recognition of the firm's commitment to delivering an excellent service to our clients and legal expertise, ByrneWallace LLP has been awarded a number of national and international awards over the years.

www.byrnewallace.com

BYRNE WALLACE LLP

International Comparative Legal Guides

The **International Comparative Legal Guide** (ICLG) series brings key cross-border insights to legal practitioners worldwide, covering 58 practice areas.

Data Protection 2024 includes two expert analysis chapters and 31 Q&A jurisdiction chapters covering key issues, including:

- Relevant Legislation and Competent Authorities
- Definitions
- Territorial and Material Scope
- Key Principles
- Individual Rights
- Children's Personal Data
- Registration Formalities and Prior Approval
- Appointment of a Data Protection Officer
- Appointment of Processors
- Marketing
- Cookies
- Restrictions on International Data Transfers
- Whistle-blower Hotlines
- CCTV
- Employee Monitoring
- Data Security and Data Breach
- Enforcement and Sanctions
- E-discovery/Disclosure to Foreign Law Enforcement Agencies
- Trends and Developments

The International Comparative Legal Guides are published by: glg Global Legal Group